

REMARKS

This is in full and timely response to the above-identified Office Action. The above listing of the claims replaces all prior versions, and listings, of claims in the application. Reexamination and reconsideration in light of the proposed amendments and the following remarks are respectfully requested.

Rejections under 35 USC § 103

- 1) The rejection of claims 1-5, 7-14 and 16-18 under 35 USC § 103(a) as being unpatentable over Gohl in view of Aziz, is respectfully traversed.

Before dealing with the specifics of the rejection, it is submitted that the person of ordinary skill in the art "thinks along the lines of conventional wisdom in the art and is not one who undertakes to innovate *Standard Oil Co. v American Cyanamid Co.*, 227 USPQ2d 293, 298 (Fed. Cir. 1985)

It is further submitted that, in order to establish a *prima facie* case of obviousness, it is necessary to show that the hypothetical person of ordinary skill would, without any knowledge of the claimed subject matter and without any inventive activity, be motivated to arrive at the claimed subject matter given the guidance of the cited references when each is fully considered as statutorily required.

In connection with motivation, there are three possible sources which would lead the hypothetical person of ordinary skill to combine references: the nature of the problem to be solved; the teachings of the prior art; and the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457-58 (Fed. Cir. 1998)

This case law, however, establishes that, even if the combination of the references may possibly teach every element of the claimed invention, without a motivation to combine, a rejection attempting to establish a *prima facie* case of obvious must be held improper. Additionally, the level of skill in the art cannot be relied upon to

provide the suggestion to combine references. *AI-Site Corp. v. VSI Int'l Inc.*, 174 F.3d 1308, 50 USPQ2d 1161 (Fed. Cir. 1999).

In more detail, it is submitted that the disclosure of Gohl has been mischaracterized. More specifically, the rejection states that Gohl “discloses providing user access via interaction with a casual application (see for example) . . .” However, the abstract of Gohl is such as to set forth:

A method and apparatus are described that authenticates a first terminal to a second terminal. In one embodiment, the invention includes, **requesting a string from the second terminal**, obtaining the requested string from the second terminal, **merging the obtained string with a password to create an identification code**, receiving an authentication if the **identification code matches an identification code expected at the second terminal** and sending information from an information server to the authenticated first terminal. In a further embodiment, the string is a pseudo random number sequence and an element of an ordered series. Merging the string can include merging the string with the password using an applet at the first terminal, the applet executing an encryption algorithm with a unique merging key. (Emphasis added)

It is submitted that this would not suggest to the hypothetical person of ordinary skill the situation wherein user access using a casual access application is carried out. To the contrary, this would suggest the opposite of casual and a situation wherein dedicated absolutely secure communication (cf. casual communication) between two terminals is intended. Attention is also called to paragraphs [0017] – [0020] wherein the tenor of the security disclosure is anything but casual. Indeed at paragraph [0031] it is set forth that:

[0031] After the user enters the user password, the client's applet asks the server through the browser for a merge string 54. The user password can be sent to the identification server at that time, **but for increased security**, it will be temporarily stored **only** at the client. If a cgi (common gateway interface) script is used, this is done by calling a cgi-script which creates a pseudo-random string of a particular length. The creation of the **pseudo-random merge string** is discussed in more detail below. (Emphasis added)

In paragraph [0031] it is set forth that:

[0032] After the **merge string** is created, it is sent from the identification server to the client 56 and then **merged at the client with the client's unique user password**. The merged string and user password becomes the identification code that is used to authenticate the client. The merge string can be sent to the client encrypted or unencrypted. **For improved security, the merge string is sent just once during the validity of the unique user password**. If it is sent often, the merge string **might be discovered by a hostile entity** by repeatedly calling the identification procedure until an identification string is received. The identification string could be used to determine the merge string and then to log in to the network. Merging is discussed in more detail below. The merging is done by the applet resident on the client. In one embodiment, as discussed in greater detail below, the merge function is one to one, and it is designed to make it very difficult to calculate an inverse. (Emphasis added)

Thus, it is clear that the hypothetical person of ordinary skill would be impressed with the level of security which is provided by Gohl and would not be moved in the least to look to disclosure such as found in Aziz "in order to provide secure access to user passwords" which is alleged to be the motivation that would drive the hypothetical person of ordinary skill to consider the teachings which are found in Aziz. Besides, as noted above, Gohl already establishes a secure password. This, it is submitted, would dampen any notion of the need to seek out techniques such as disclosed in Aziz in order to redundantly and possibly less securely prevent unauthorized access to the password or passwords in question.

Applicants also call attention to the fact that Aziz discloses in connection with the flow chart which is shown in Fig. 4, that there is an enquiry as to whether a user is on a "list" of "authorized" users. If there is a list of authorized users then this disclosure cannot be taken as being particularly pertinent to "casual" access, and in fact would suggest that the intentions of Aziz are as formalized as those of Gohl, and therefore such as to teach away from a casual /non-casual stratification in access priority.

In this connection the assertion that Gohl discloses generating and transmitting an external message to a "casual" user, is traversed.

The instant specification defines "casual" in the sense that it is used in this application as follows:

A casual user is defined as one who may not need full access to the exchange and its applications, but may only need to complete simple business transactions. For example, an organization may be a member of the exchange via the membership of its procurement employee. Under that organization's policies, the procurement employee is authorized to make purchases on behalf of the organization for under a certain amount. If the cost of a purchase is over that certain amount, it is necessary for that procurement employee to get additional

authorization from his or her manager. This manager, however, may not be registered to participate in the electronic exchange or to use its applications. In order to complete the transaction, that manager's authorization is necessary. Thus, it is desirable to allow the manager to have access as a casual user for the limited purpose of providing the necessary authorization.

In addition, the only mention of the term "casual" in either of Gohl and Aziz is found in Aziz:

In the following description, numerous details are set forth such as workstation system configurations, representative messages, servers, etc., to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well known circuits and structures are not described in detail in order to not obscure the present invention. Moreover, certain terms such as "knows", "sends", "receives", "verifies", "examines", "finds", "determines", "authenticates", etc., are used in this Specification and are considered to be terms of art. The use of these terms, which to a **casual reader** may be considered personifications of computer or electronic systems, refers, for simplicity, to the functions of the system as having human-like attributes. For example, a reference herein to an electronic system as "determining" something is simply a shorthand method of describing that the electronic system has been programmed or otherwise modified in accordance with the teachings herein. The reader is cautioned not to confuse the functions described

with everyday human attributes. These functions are machine functions in every sense. (Emphasis added)

Irrespective of the fact that the Applicants have acted as their own lexicographer, given the instance wherein (*arguendo*) this is ignored and the meaning of casual as used in the claims is given its absolute broadest interpretation, reference is made to following dictionary definition:

The American Heritage® Dictionary of the English Language: Fourth Edition. 2000.

casual

ADJECTIVE: 1. Occurring by chance.

As will be appreciated, the claims by calling for a casual user immediately leads away from the “formalized” nature of being on a “list of authorized users” – see first step on flow chart in Fig. 4 of Aziz, and the string merging techniques disclosed in Gohl. It is immediately self-evident that none of the processes which are disclosed in Gohl and Aziz are apt to “occur by chance” and therefore cannot be taken as suggesting “casual user access” by a “casual user” using a “casual access application” within the meaning of casual as defined either in the specification or by dictionary.

Irrespective of the above, the combination of Gohl and Aziz is not seen as resulting in a *prima facie* case of obviousness in that, as noted above, the motivation to use a technique (such as found in Aziz) which could readily be perceived as providing a lower level of security than that already available in Gohl, would not normally result when the disclosure of the two references are considered as a whole.

On page 9, paragraph 14, of this Office Action, the position is taken that ‘Gohl meets the limitation “receiving a request from an external application”.’ (Emphasis added) This suggests an anticipation under § 102 type of approach of reading the specifications of Gohl and Aziz and is not consistent with the requirements which must be met in establishing a *prima facie* case of obviousness under 35 USC § 103. This

position pervades both rejections. Indeed, as pointed out above, the abstract contains nothing that would suggest that the arrangement disclosed in Gohl is directed to providing user access via interaction with a casual access application.

In the paragraph spanning pages 2 and 3, of this Office Action, it is asserted that the step of generating a context-sensitive CS-PIN upon access of said casual application by said casual user using said information – is disclosed/suggested by paragraphs 31 and 45 of Gohl. However, these paragraphs of Gohl respectively disclose:

[0031] After the **user enters the user password**, the client's applet asks the server through the browser for a merge string 54. The **user password** can be sent to the identification server at that time, but for increased security, it will be temporarily stored only at the client. If a cgi (common gateway interface) script is used, this is done by calling a cgi-script which **creates a pseudo-random string of a particular length**. The creation of the pseudo-random merge string is discussed in more detail below.

[0045] As shown in FIG. 3, the user password is fetched from a register 80 where it is stored in an **encrypted form**. It is then encrypted in the same or another way 82. Alternately, the **encryption** that is already applied in the register 80 can be used. These encryption functions are controlled by the applet and more or less encryption can be applied as desired. Similarly, the **merge string is fetched from another register** 84 where it is stored in an encrypted form. It is then encrypted again 86. Alternatively, since the merge string is a pseudo-random sequence with a shorter term validity, it can be stored unencrypted and applied to the merge function without encryption or as with the user password, it can be used in the form in which it is

stored. The **two elements are then merged** 88 and the **result is encrypted** 90. The encrypted result can be used as the identification code 94 that is used to authenticate all of the communications that follow. The merge function can be a simple block addition. Such a simple block addition can be expressed as follows:

`newString[i]=encryptedRandomString[i]+passwordString[i].`

It is respectfully submitted that this is a step beyond just generating a CS-PIN upon access of a casual application and would not be seen by the hypothetical person of ordinary skill as such.

In this response, it is proposed, in light of the comments set forth under the heading of “Response to Arguments” (paragraph #14) concerning the “external application” and the rebuttal that Gohl does in fact disclose “receiving a request from an external application” to the degree that paragraph [0028] of Gohl, discloses a “request page” and that this is depicted in Fig. 3; to clarify the claimed subject matter by proposing amendments to claims 1 and 9, which call for an event to be detected in the electronic exchange by an electronic exchange application. It is clear that this is different from the casual user and that the confusion which has lead to the above, is clarified by this amendment. It is also submitted that neither of Gohl or Aziz disclose or suggest the detection of this event within an electronic exchange application.

More specifically, Fig. 3 of Gohl contains no mention of either of “request” or “page” and paragraph [0028] of Gohl discloses:

[0028] To begin a session, the client sends a **request** to the identification server 50. This is typically answered by sending an HTML document back to the client 52. Before the session begins, the client can be initiated. To do this, a special program can be sent to and loaded onto the client machine that tracks passwords and encryption keys and

performs the various encryption operations discussed herein. In one embodiment, this program is a log in applet written in Java for use with the Netscape Navigator internet browser, however other browsers including Microsoft Internet Explorer can be used instead. The log in applet works with a user password to log in the user for the session. In this embodiment, the communications discussed below occur over the internet with a server through the browser. The applet is transmitted from the server to the client over the internet as is well-known in the art. The user password can also be transmitted either from the server or to the client over the internet, however, the user password can be handled with more security. A variety of different security schemes including SSL, discussed above, can be applied to the log in applet and user password transactions. (Emphasis added)

While this passage mentions the client sending a “request” to the ID server, there is no mention or suggestion of the detection of an event within an electronic exchange application which prompts the generation and transmission of an external message.

It is therefore submitted that the amendments proposed to claims 1 and 9 both clarify issues and overcome the rejection under 35 USC § 103(a). For this reason it is submitted that they should be considered and entered for at least this reason.

2) The rejection of claims 6 and 15 under 35 USC § 103(a) as being unpatentable over Gohl, Aziz and further in view of Sormunen et al. (Sormunen), is respectfully traversed.

In this rejection it is acknowledged that “the combination of Gohl and Aziz does not explicitly teach the CS-PIN holding being an email address accessible by both the casual access application and the casual user”. To overcome this admitted

shortcoming it is submitted that "any means of holding the CS-PIN to be transmitted to the external application can be used" and Sormunen is then cited to show that the generation of a CS-PIN and a CS-PIN holder which are accessible by both the casual access application and the casual user. Examples of ID and password usage on "hotmail" and "yahoo" mail are given.

However, this overlooks the technique which is disclosed in Gohl and fails to establish a *prima facie* case as to why the hypothetical person of ordinary skill would look to Sormunen for teachings in light of those which are already provided by both Gohl and Aziz.

Conclusion

It is respectfully submitted that a *prima facie* case of obviousness has not been established and that the claims as they stand before the Patent and Trademark Office are allowable even absent the clarifying amendments which are proposed in this response. Favorable reconsideration, entry of the clarifying amendments and allowance of this application are therefore courteously solicited.

Respectfully submitted,

By



Date March 31, 2005

FOLEY & LARDNER LLP
Customer Number: 22428
PATENT TRADEMARK OFFICE
Telephone: (202) 672-5485
Facsimile: (202) 672-5399

William T. Ellis
Registration No. 26,874

Keith J. Townsend
Registration No. 40,358